Passive IP Address draft-baker-opsec-passive-address-01.txt

Fred Baker

Gunter Van de Velde

Diff between -00 and -01

- Added usage case for Passive address regarding LL-only network environment to regain operational limited network visibility
- Clarified that a passive address is just as a traditional address, but that if a device receives a message with such a IP address in the destination field that it is dropped
- Clarified that semantics between traditional IP address and passive address is identical

What are they?

- Passive IP addresses do not increase network obscurity, but do harden the security on the network
- It are addresses from the normal global/ULA pool of addresses
- A potential usage case: passive addresses could contribute to operational network visibility in a LL-only infrastructure… it provides trace-route capability
- A passive address does not need new or special address space
- Passive address can NOT be used in an IP packet as a DESTINATION address, however only as SOURCE address. (this results in the artifact that a passive IP address CAN NOT be ping'd for example)

A potential usage model

- Assume a router is configured with:
  - A traditional /128 loopback address on a loopback (mainly used for telnet/ssh to the device and for potentially OSS/Management)
  - Passive addresses on other interfaces
  - LL on other interfaces
  - Global IP address on the device loopback
- For device management/maintenance the loopback of the device is used
- When a packet goes through the router and for example ttl expires (trace-route), then ICMP message ttl-expired can be returned with the interface where ttl expired. (trace-route works again)
- The recipient of this ttl-expired message can not use the IP address to reach or attack the router, because the router will simply drop the packet